Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)
Enterprise Risk Management Office

Access Management Standard

Document Name: Access Management Standard	Effective Date: October 15th, 2018
Document ID: IS.014	Last Revised Date: March 5, 2025

Table of Contents

1. PURPOSE

1.1. **Access Management** — This ***standard*** defines the requirements for protecting the Commonwealth's ***information assets*** throughout their life cycle from the original request for access to the revocation of privileges. This ***standard*** addresses the following:

1.1.1. ***User*** access management to verify authorized ***user*** access to ***information assets***

1.1.2. ***User*** password management to control allocation of account passwords

1.1.3. ***User*** responsibilities to prevent unauthorized access and compromise of ***information assets***

1.1.4. Network access control to verify the security of network services and information assets

1.1.5. System authentication control to verify authorized access to ***information assets***

1.1.6. Provisioning of contractors' access to ***information assets*** through a formal management process

2. AUTHORITY

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security, (EOTSS), possess the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of ***information, information systems***, ***assets***, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, ***agencies***, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), by any form of contractual arrangement, are required to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***standard***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***standard*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. Additional ***information*** regarding this ***standard*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/***policies*****.**

4.3. In the event of any conflict between the provisions contained in this ***standard*** and the provisions set forth in any of the Enterprise Information Security Policies, the provisions in the Enterprise Information Security Policies will govern.

4.4. Definitions of terms in bold may be found in the ***IS.Glossary of Terms*** at https://www.mass.gov/cybersecurity/***policies.***

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance

5.3.2. Identify and explain in detail the ***risks*** created due to the non-compliance

5.3.3. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level

5.3.4. Specify the time-frame required to implement the ***controls*** and mitigate the identified ***risks***. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact information for both the ***risk owner*** and the ***control owner*** designated by the agency to accept and manage the ***risks*** associated with the non-compliance and implement the ***controls*** that will effectively mitigate the identified ***risks***.

6. STANDARD STATEMENTS

6.1. USER AND SYSTEM ACCESS MANAGEMENT

6.1.1. ***User*** or system access will be managed throughout the account life cycle from the identification of a ***user*** to the granting, modification or revocation of a ***user's*** access privileges.

6.1.2. <u>Allowed Access Types</u>: Access by Commonwealth accounts fall under the following categories:

6.1.2.1. <u>Privileged Access</u>: Any account type that grants ***users*** elevated or increased ***application*** or ***information system*** capabilities that may affect computing systems; network communication; or the accounts, files, ***data***, or processes of Commonwealth systems, including the ability to read, update or distribute highly ***sensitive information*** or make changes to system configurations and security settings.

6.1.2.2. <u>Interactive Access</u>: Any account type that allows one individual to log into an ***information system***, through either a remote or direct connection, by entering appropriate credentials and supplying commands.

6.1.2.3. <u>Non-Interactive Access</u>: Any account type (i.e., non-human) used solely by a process, service, or ***application*** to communicate with other systems.

6.1.2.4. <u>Shared Access</u>: Any account type that is shared by two or more ***users*** or systems and may or may not provide the ability to associate a login or activity with a particular ***user*** or system (e.g., built-in account).

6.1.2.4.1. The creation and/or existence of non-built-in shared accounts must be managed using a formal ***risk*** management ***process,*** and the submission of a policy non-compliance report, as detailed above.

6.1.2.4.2. All policy non-compliant shared account access should be time-boxed (where technically feasible), and the use of passwords should be controlled with an approval (e.g., Enterprise Security Office or agency ***CISO***) driven checkout process.

6.1.2.4.3. Passwords should be changed regularly and whenever a shared account member is removed from group access (see *Password Management in IS.014 Access Management Standard*).

6.1.3. Allowed Account Types: Allowed Commonwealth accounts fall under the following categories:

6.1.3.1. ***User*** Account: A unique ID or login account owned by a single individual.

6.1.3.2. Administrator Account: A privileged interactive account that is assigned to one and only one ***user***. Passwords for these accounts must not be shared. Administrator accounts provide individuals with a frequent need for elevated access to have the associated privileges and segment their regular access from the administrative access.

6.1.3.3. System Account: A built-in account that enables administration, communications or processing services within infrastructure systems, platforms, ***applications***, and databases. Some system accounts are not intended for regular active use and control by ***users*** and are simply in place to start and stop various processes.

6.1.3.4. Service Account: Interactive or non-interactive accounts that are not built in but are put in place by an organization to enable functionality such as communications or processing services within and between infrastructure systems, platforms, ***applications***, and databases. These types of accounts may also be used to grant specialized elevated rights to ***applications***, systems, or shared mailboxes.

6.1.3.5. Firecall (or Breakglass) Account: Interactive accounts with temporary privileged access rights that are intended for use on production systems by human ***users*** during operational, maintenance and troubleshooting activities.

6.1.3.5.1. Firecall accounts are managed via an automated or manual check-out process that requires an approved change control, service ticket, or other tangible business justification. Firecall accounts enable management of the environment and limit the need to directly access system accounts.

6.1.4. Prohibited Account Types: Prohibited Commonwealth accounts fall under the following categories:

6.1.4.1. Shared Accounts: The creation and/or existence of non-built-in shared accounts is prohibited unless managed using a formal ***risk*** management ***process,*** and the submission of a policy non-compliance report, as detailed above. All policy non-compliant shared account access should be time-boxed (where technically feasible), and the use of passwords should be controlled with an approval (e.g., Enterprise Security Office or agency ***CISO***) driven checkout ***process***. Passwords should be changed regularly (see Password Management in *IS.014 Access Management Standard*).

6.1.5. Privileged Access Management: Where technically feasible (and available), certain types of privileged accounts will be managed by a privileged access management (PAM) solution, maintained, or approved by the Enterprise Security Office, or manual process, as follows:

Account type	Interactive	Shared	Control and Usage
Administrator	Yes	No	Administrator accounts are generally allocated to individuals; their use needs to be constrained by strong security policies. • PAM functionality: Not required although process to audit account access should be implemented • Example/use: account used to reset passwords
Service (a)	Yes	Yes	Service accounts have elevated rights but should generally not be shared unless required by business or technical constraints. • PAM functionality: Strong passwords, centrally manage passwords; password rotation • Example/use: Oracle DB account used to read ***data***; accounts configured to enable particular functionality; accounts used to read ***log*** directories or manage group email lists
Service (b)	No	No	• PAM functionality: Enhanced monitoring • Example/use: Accounts used strictly for system-to-system calls to support regular operations
System (a)	Yes	Yes	The applicable ***controls*** required for system accounts are highly dependent on the operational nature of an ***application***, the technical constraints, and underlying technology and/or vendor restrictions. • PAM functionality: Check-in, check-out; complex passwords; password rotation; and enhanced monitoring

			• Example/use: Sys DBA for Oracle; Root access for Unix (sudo)
System (b)	No	No	Some system accounts are non-interactive and do not allow login. • PAM functionality: Strong password (if applicable); enhanced monitoring • Example/use: accounts used strictly for system-to-system communication, potential use of certificate or key-pairs
Firecall	Yes	Yes	Firecall accounts are not allocated to individuals and are generally managed by a check-in/check-out process and should also have strong passwords and increased monitoring. • PAM functionality: Check-in, check-out; password rotation; time-limit access • Example/use: emergency and temporary access to Production environments

6.1.6. Request Access Privileges

6.1.6.1. ***User*** requests for access privileges will follow a formal process.

6.1.6.2. Commonwealth Agencies and Offices must ensure that ***personnel*** sign and agree to the *Acceptable Use* Policy prior to obtaining any system access (*see IS.002 Acceptable Use Policy)*.

6.1.6.3. ***User*** registration and revocation procedures will be implemented for all ***information systems*** and services.

6.1.6.4. ***User*** access requests will be recorded (paper or tool-based), include a business justification for access, and be approved by the requestor's supervisor and the appropriate ***Information Owner*** or authorized delegate.

6.1.7. Grant Access Privileges

6.1.7.1. Commonwealth Agencies and Offices must ensure that ***Personnel*** with security administration roles (hereafter, "***security administrators***") are responsible for the creation of accounts and the assignment of privileges after receiving the required access approvals.

6.1.7.2. Account Managers: The ***Security Administrators*** perform the role of account managers for ***user*** access by creating, modifying, and revoking accounts, as well as serving as the point of contact for communications when ***user*** access needs change.

6.1.7.3. Access Authorization: The ***Information Owner*** or ***Information Custodian*** will verify that the type of access requested is required for the ***user's*** role and responsibilities.

6.1.7.4. Least Privilege: Access will be granted using the principle of least privilege, i.e., a ***user*** will only receive the minimum level of access and/or permissions required to perform his or her job responsibilities.

6.1.7.5. Segregation of Duties: The ***Information Owner*** will confirm that conflicting access is separated to prevent fraud and/or misuse of the organization's ***assets***.

6.1.7.6. Group and Role Membership: The ***Security Administrators*** will determine the appropriate group and role membership of a ***user*** in the system based on the access request.

6.1.8. Modify Access Privileges

6.1.8.1. Upon the need for a change of ***user*** access, Commonwealth Agencies and Offices must ensure that a ***user*** access change request is recorded.

6.1.8.2. The change request must be submitted to EOTSS online through ServiceNow, https://www.mass.gov.service-now.com by the agency's IT Liaison, (ITL).

6.1.8.3. The change request should include a business justification for the change in access and must be approved by both the requestor's supervisor and the appropriate ***Information Owner*** or authorized delegate.

6.1.8.4. Account managers must be notified when system usage or need to know changes for an individual.

6.1.9. Revoke Access Privileges

6.1.9.1. Upon a transfer, termination or other significant change to a ***user's*** employment status or role, the ***user's*** previous supervisor is responsible to inform security administration personnel, so they may take appropriate action.

6.1.9.2. Account managers will be notified when accounts are no longer required, when ***users*** are terminated, when ***users*** are transferred, and when system usage or need to know changes for an individual.

6.1.9.3. Privileges that are no longer required by a ***user*** to fulfill his or her job role will be removed.

6.1.9.4. If the termination date of a ***user*** is known in advance, the respective access privileges — specifically those with access to ***confidential information*** — will be configured to terminate automatically. If not, access must be manually removed within 24 business hours.

6.1.9.5. ***Security administrators*** in consultation with the Enterprise Security Office (or agency's ***Information Security Team***) may temporarily suspend or restrict a ***user's*** level of access to the network if his or her account is suspected of privilege abuse or violation of the *Acceptable Use* policy, (see *IS.002 Acceptable use of Information Technology Policy*).

6.1.10. Monitor Use of Accounts

6.1.10.1. Account activity will be monitored and reviewed in accordance with *IS.022 Logging and Event Monitoring Standard*.

6.1.10.2. Review of ***user*** access rights: Commonwealth Agencies and Offices must ensure that ***security administrators*** maintain and review account access (either tool-based or manual) to verify that inactive and unauthorized accounts are appropriately de-provisioned.

6.1.10.3. Audit ***logs*** for account creation/ modification, deletion and access change will be retained and reviewed in accordance with *IS.011 Logging and Event Monitoring Standard*.

6.1.10.4. A review of ***user*** access must be conducted, at a minimum, semiannually, and all unauthorized accounts and access must be removed.

6.1.10.5. Login accounts inactive for 90 days must be disabled.

6.1.10.6. Disable accounts for ***personnel*** scheduled to go on an extended leave of absence of more than 90 days.

6.1.10.7. Remove or disable ***user*** accounts that no longer require access to ***information assets***.

6.1.10.8. Revoke access for any ***user*** no longer employed or under contract with a Commonwealth Agency or Office within 24 hours of notice.

6.1.10.9. More frequent reviews are encouraged commensurate to the ***risk*** level of the ***information asset*** or to meet regulatory requirements.

6.1.10.10. Privileged access reviews for Critical and High rated ***information*** systems will be conducted by the ***Information Custodian*** or authorized delegate on a quarterly basis.

6.1.10.11. More frequent reviews are encouraged commensurate with the ***risk*** level of the ***information asset*** or to meet regulatory requirements.

6.1.10.12. On a periodic basis, Commonwealth Agencies and Offices will align account management ***processes*** with the ***personnel*** termination and transfer ***processes***.

6.1.11. Manage Privilege Access for System Utilities

6.1.11.1. Access to system tools that have the capability to override system and ***application controls*** will be restricted by Commonwealth Agencies and Offices to authorized ***personnel***. All access to system utilities and tools will be logged to facilitate the investigations of inappropriate use.

6.1.11.2. Privileged accounts (e.g., root or administrator level accounts) will be used only for system administration where such access is required.

6.1.11.3. Administrative accounts will not be used for non-administrative purposes (e.g., browsing the Internet).

6.1.11.4. Privileged ***user*** access will be logged and monitored to prevent misuse of ***information assets***.

6.1.12. Emergency Access Management

6.1.12.1. Procedures will be established and implemented as needed, to obtain necessary access to ***information assets*** during an emergency in accordance with *IS.016 Business Continuity and Disaster Recovery Standard*.

6.2. ACCOUNT MANAGEMENT

6.2.1. Commonwealth Agencies and Offices will document and implement proper ***user*** identification and authentication ***processes***, including:

6.2.1.1. ***Control*** and ***log*** the addition, deletion and modification of ***user*** IDs, credentials, and other identifier objects.

6.2.1.2. Verify ***user*** identities prior to allowing password resets.

6.2.1.3. Require the use of a unique ID and ***multi-factor authentication*** for system administration and other privileged access, including the management of network devices or ***information systems*** that contain ***confidential information***, and for remote ***user*** access.

6.2.1.4. Disallow use of personal ***user*** accounts for administrative activities; as well, do not use administrative accounts for personal use.

6.2.1.5. Time-box and monitor accounts used by ***third parties*** for remote access.

6.2.1.6. Disconnect remote-access sessions after a specified period of inactivity (no longer than four (4) hours).

6.2.1.7. Restrict access to any database containing ***confidential information*** (including access by ***applications***, administrators, and all other ***users***) by:

6.2.1.7.1. Limiting ***user*** access to, ***user*** queries of and ***user*** actions on databases to programmatic methods.

6.2.1.7.2. Limiting the ability to directly access databases containing ***confidential information*** to only database administrators and only for administrative purposes.

6.2.1.7.3. Limiting the use of ***application*** IDs for database ***applications*** to ***application*** processes (i.e., non-interactive).

6.2.1.8. Access attempts will be limited by locking ***user*** IDs after no more than five (5) failed login attempts.

6.2.1.8.1. In the event a ***user*** account is locked out, the ***user*** must call the IT service desk to re-enable account access.

6.2.1.8.2. A self-service password reset function managed and monitored by the Enterprise Security Office may be used.

6.2.1.8.3. “Reset account lockout counter after” policy will be set to 30 minutes to mitigate against password timing and guessing attacks.

6.3. INFORMATION SYSTEMS

6.3.1. ***Information systems*** (e.g., operating systems, databases, and ***applications***) will be configured with appropriate authentication ***controls*** designed to prevent unauthorized disclosure, modification, or access to ***information***.

6.3.2. Remote, wireless, and mobile access will only be allowed for employees and contractors with a valid authorization and will be provisioned by Security Administrators in alignment with approved configurations.

6.3.3. No system or database containing non-published ***information*** will be directly accessible from an untrusted network or ***information system***.

6.3.4. Logon processes will be customized wherever possible to display only the ***information*** required for the ***user*** to authenticate. Minimal ***information*** about the ***information system*** will be disclosed to avoid providing an unauthorized ***user*** with contextual ***information***.

6.3.5. Workstations left unattended for extended periods of time must be locked or logged off.

6.3.6. The time-out delay will reflect the security ***risks*** of the system, the classification of the ***information*** being handled, and the ***risks*** related to the ***users*** of the system.

6.3.7. An automatic screen saver lock will be configured to become active no more than five (5) minutes after inactivity for workstations used by ***personnel*** with access to any Commonwealth network and ***information system***.

6.3.6 Put devices into a sleep or locked mode any time they are not in active use.

6.3.7 Network devices and systems will be configured with appropriate access ***controls*** to prevent unauthorized modification or access to ***information assets*** and internal and external networked devices (See *Network Security Management in IS.017 Communications and Network Security Standard*).

6.3.8 Other than use of publicly available websites and systems, no ***user*** actions may be performed within systems without identification and authentication of the ***user***.

6.4. PASSWORD MANAGEMENT

6.4.1. Commonwealth Agencies and Offices must ensure that systems and processes to manage the enforcement of password ***controls*** for access to the network, operating systems, databases, or ***applications*** will be interactive and require strong passwords.

6.4.2. Passwords will be configured securely using complexity and expiration requirements, as follows:

6.4.2.1. ***User*** passwords must be a minimum of twelve (12) characters and contain three (3) of the following four (4) characteristics:

6.4.2.1.1. Special characters (e.g., ‘, %, $, #)

6.4.2.1.2. Numerical characters (e.g., 1, 2, 3)

6.4.2.1.3. Alphabetic characters (e.g., a, b, c)

6.4.2.1.4. Combination of uppercase and lowercase letters

6.4.2.2. Passwords will not use repeating, ascending, or descending character sequences (e.g., 12345, or abcde).

6.4.2.3. Passwords will not use common words found in a dictionary, contain any part of a ***user's*** name, or the organization's name.

6.4.2.4. The use of a "passphrase" is recommended, such as: *Tcopire2d!* – A passphrase that is easy to remember as the cracking of passwords is sometimes very easy.

6.4.2.5. Passwords will not be the same as any of the last nine previously used passwords.

6.4.2.6. Privileged accounts (e.g., administrator) passwords must consist of a minimum of fifteen (15) characters and contain the four (4) characteristics mentioned above.

6.4.2.6.1. If the system is limited to less than fifteen (15) alphanumeric characters, then the administrator's password length must be set to the maximum number of characters allowed by the operating system or ***application***.

6.4.2.6.2. If it is less than eight (8) alphanumeric characters, a policy non-compliance report must be submitted to the ERM office for review by the ***Commonwealth CISO***.

6.4.2.7. For instances of ***multi-factor authentication, user*** defined Personal Identification Numbers (PINs) must be a minimum length of at least eight (8) characters. This PIN will be used in conjunction with a six-digit randomly generated token PIN.

6.4.2.7.1. Authentication mechanisms (e.g., hard, or soft tokens) must be assigned to an individual account and not shared among multiple accounts.

6.4.2.7.2. Physical and/or logical ***controls*** must be in place to confirm that only the intended account can use that mechanism to gain access.

6.4.2.8. Password must expire or change, as follows:

6.4.2.8.1. Require change of initial (or temporary) password upon first-time login/use. Initial passwords must be unique for each ***user*** and received in a secure manner.

6.4.2.8.2. Passwords/PINs must be changed immediately if a compromise is suspected.

6.4.2.8.3. ***User*** accounts must be changed at least once every 180 days and administrator accounts must be changed at least once every 90 days.

6.4.2.8.4. Enforce a minimum password age of at least one (1) day.

6.4.2.8.5. Service account passwords must be changed at least annually.

6.4.3. PINs used with approved ***multi-factor authentication*** solutions do not have to be regularly changed. Passwords for IDs used for non-interactive system access (e.g., IBM Mainframe batch IDs, Microsoft Windows service accounts or password disabled Unix IDs) may be exempt from the 90-day password change requirement. The system-specific technical standards will be referenced for additional and/or qualifying ***controls***.

6.4.4. Commonwealth Agencies and Offices must ensure that one-time use and temporary passwords must adhere to the following:

6.4.4.1. Passwords must not be sent via fax.

6.4.4.2. Passwords must not be sent via email unless the email is ***encrypted***.

6.4.4.3. Passwords must not be given via telephone unless the password administrator has positively identified the caller’s identity.

6.4.4.4. Initial or temporary passwords must be forced to be changed immediately upon their first use.

6.4.4.5. Initial passwords must comply with the password composition and password selection requirements specified in this ***standard***.

6.4.5. Commonwealth Agencies and Offices must ensure that ***security administrators*** must positively identify the identity of a ***user*** prior to a password reset.

6.4.5.1. Only the individual to whom the ***user*** ID is assigned may request a password reset.

6.4.5.2. Password resets will not be performed prior to verification of the requestor's identity.

6.4.5.3. If a self-service portal is not available, a "reset" password will function as a one-time password required to be changed upon first use or login.

6.4.6. A ***user*** ID and password will be authenticated in its entirety. If authentication fails, the system error message will not indicate which component of the ***user's*** input (***user*** ID or password) is incorrect (e.g., "incorrect login," or "incorrect password").

6.4.7. Passwords usage and storage must be secure.

6.4.7.1. Default passwords for ***software*** or hardware will be disabled or changed.

6.4.7.2. Where technically feasible, password filtering and password masking will be implemented.

6.4.7.3. Password credentials must be ***encrypted*** and will never be transmitted in clear text.

6.4.7.4. Password files must be stored in an ***encrypted*** form separate from the object or ***application data*** they protect.

6.4.7.5. ***Users*** must not share or reveal passwords to anyone.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 18 v8	NIST CSF
7.1 User and System Access Management	AC-1	-	ID.GV-1
	AC-2	CSC 5	PR.AC-1
	AC-3	CSC 5	PR.AC-4
	AC-5	CSC 5	PR.AC-4
	AC-6	CSC 5	PR.AC-4
	CM-5	CSC 4	PR.IP-1
	IA-2	CSC 16	PR.AC-1

	IA-8	CSC 16	PR.AC-1
	IA-9	CSC 16	PR.AC-1
	AC-21	-	PR.IP-8
	IA-1	-	ID.GV-1
		CSC 5	PR.PT-3
7.2 Account Management	AC-7	-	-
	AC-8	-	-
	AC-9	-	-
	AC-11	-	-
	AC-12	-	-
	AC-14	-	-
	AC-17	CSC 6	PR.AC-3
	AC-18	CSC 4	-
	AC-19	CSC 4	DE.CM-5
	IA-2	CSC 5	PR.AC-1
	IA-4	CSC 5	PR.AC-1
	IA-5	CSC 5	PR.AC-1
	IA-6	CSC 4	PR.AC-1
	IA-10	CSC 4	PR.AC-1
	IA-11	-	-
	PE-2	-	PR.AC-2
	PE-3	-	PR.AC-2
	SC-10	-	-
	AC-23	-	-
	AC-25	-	-
7.3 Password Management	IA-2	CSC 5	PR.AC-1
	IA-5	CSC 5	PR.AC-1

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.95	John Merto	12/22/2017	Edits; fixed numbering
0.96	Sean Vinck	5/7/2018	Corrections and Formatting
0.97	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O’Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Final Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto

1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	NIST 800-53R5 mapping and annual review
1.4	Thomas McDermott	10/30/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony O’Neill	10/30/2023	Final Review
1.5	Thomas McDermott	11/18/2024	Corrections, Formatting and Annual Review
1.5	Anthony O’Neill	11/18/2024	Final Review
1.6	Thomas McDermott	2/7/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	2/26/2025	Corrections and Formatting
1.6	Anthony O’Neill	3/5/2025	Final Review